ISA Delhi Section

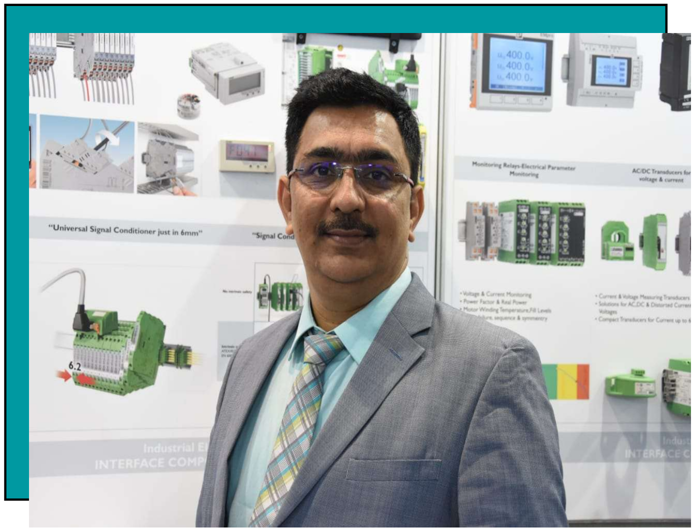
Setting the Standard for Automation™

Secured & Safe Plant Automation

By Phoenix Contact

ISA-D: “Fertiliser , Food and Pharma Symposium-2022”

May I introduce myself?



Valmik Suryavanshi
Business Development Head
Industry Management & Automation
Email: vsuryavanshi@phoenixcontact.co.in

Address:
37, Devi House, Shivaji Nagar
Pune – 411001

Office:	+91 – 20 – 305 23 636 ,30581224-231
Mobile:	+91 – 9158000672

Headquarters and Competence Center

Headquarters Blomberg/Germany

Group Center of Competence, Harrisburg/USA

Innovation Center Electronics, Bad Pyrmont/Germany

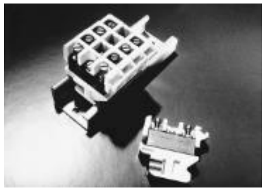
Group Center of Competence, Nanjing/China

Many years of experience

Development from 1923 to today

1923
Foundation in Essen

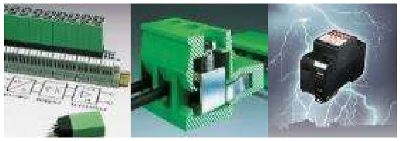
1928
The RWE terminal block



1966
Company headquarters
established in Blomberg

1967
Strip
terminal
blocks

1977, 1982 und 1983
Plug-in relay terminal
PCB terminal blocks
Surge protection



1981
Onwards: First foreign
subsidiaries

1987
INTERBUS –
serial fieldbus
system

2005
Safety

Today
Located all over
the world

PROFICLOUD

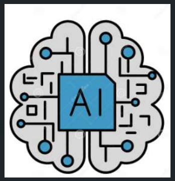
Push-in Technology
Designed by PHOENIX CONTACT

PLCnext Technology
Designed by PHOENIX CONTACT

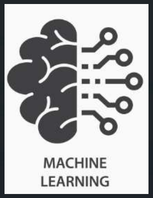
Current Trends & Challenges

Connected Devices

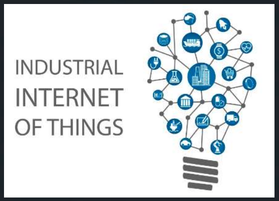
APL



IEC 62443



NOA



ISO 27001

Cloud Computing

Digital Factory | Data Security | Security evaluation

Cyber attacks have arrived in reality

#1 Corporate risk (worldwide)

Source: Allianz AG risk barometer

68% of industrial companies in Germany have already fallen victim to cyber attacks.

Source : VDMA

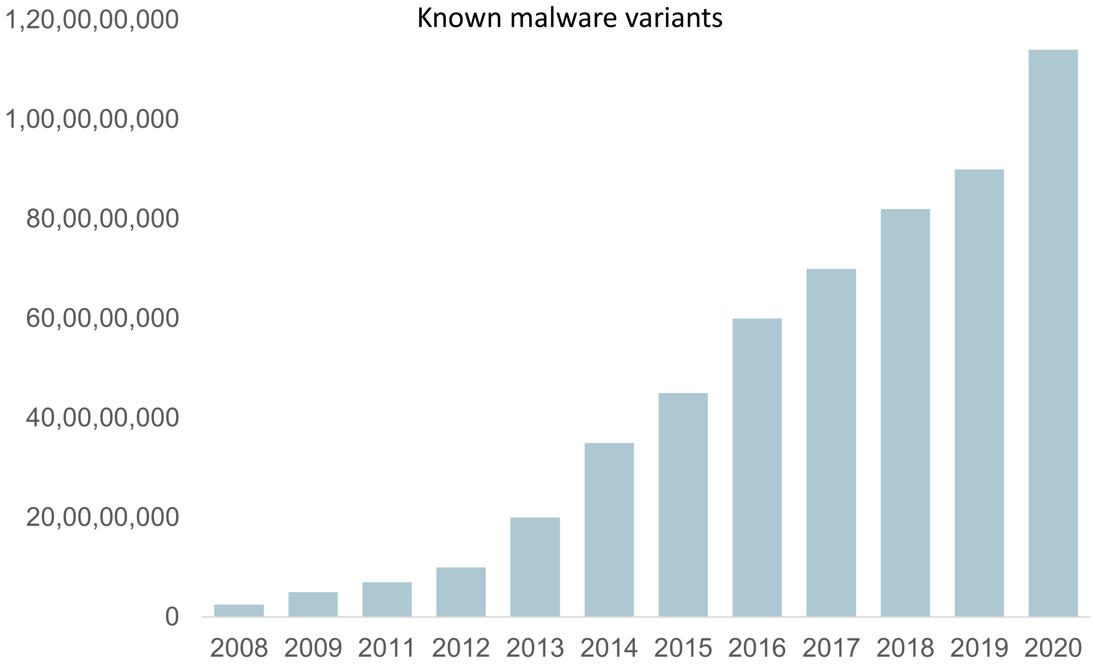
59% of these attacks lead to production losses

Source : VDMA

Digital Factory | Data Security | Security evaluation

Cyber attacks as corporate risk #1

„68% of industrial companies in Germany have already fallen victim to cyber attacks. “ (VDMA)



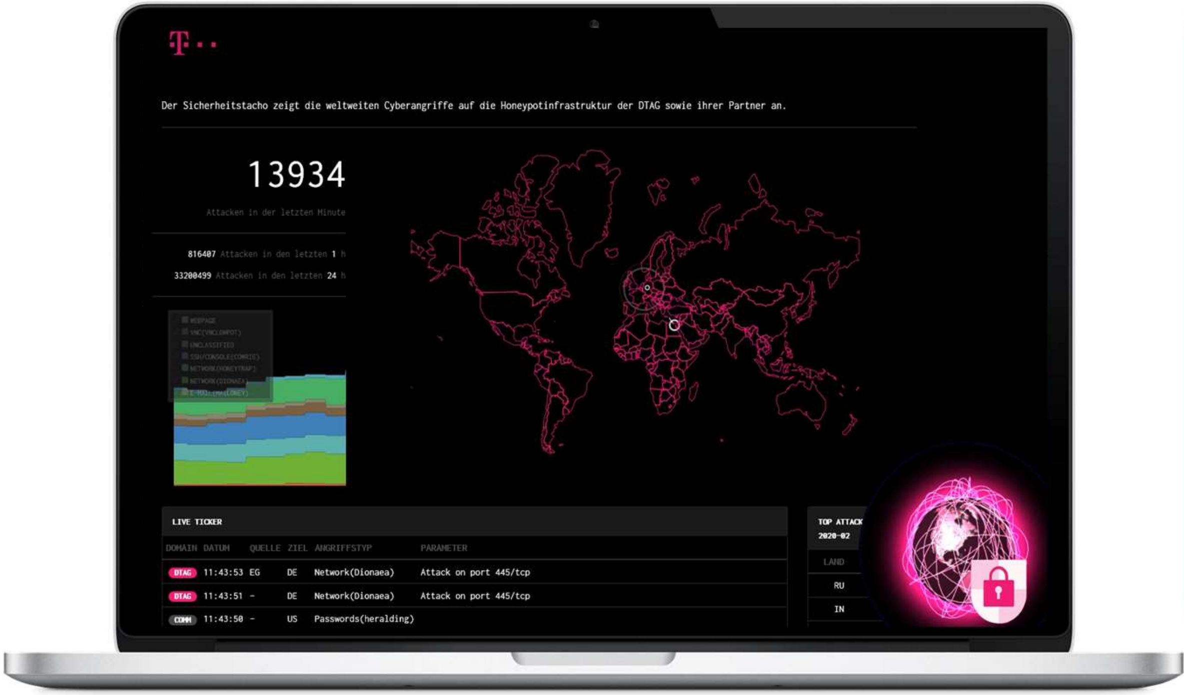
TOP 3 threats in the ICS environment:

1. Infiltration of malware via removable media and external hardware
2. Infection with malware via the Internet and intranet
3. Human misconduct and sabotage

Digital Factory | Data Security | Security evaluation

Threat situation

Online cyber attacks (Kaspersky Cyberthreat real-time map)



Der Sicherheitstacho zeigt die weltweiten Cyberangriffe auf die Honeypotinfrastruktur der DTAG sowie ihrer Partner an.

13934

Attacken in der letzten Minute

816407 Attacken in den letzten 1 h

33200499 Attacken in den letzten 24 h

LIVE TICKER

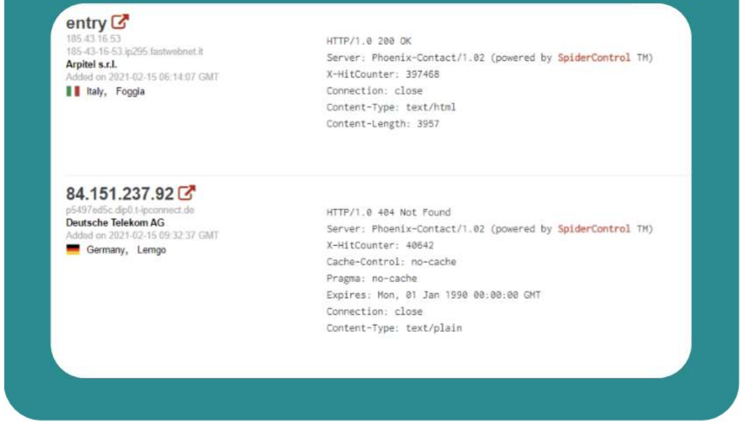
DOMAIN	DATUM	QUELLE	ZIEL	ANGRIFFSTYP	PARAMETER
DTAG	11:43:53	EG	DE	Network(Dionaea)	Attack on port 445/tcp
DTAG	11:43:51	-	DE	Network(Dionaea)	Attack on port 445/tcp
COMM	11:43:50	-	US	Passwords(heralding)	

TOP ATTACK
2020-02

LAND
RU
IN

Source: www.sicherheitstacho.eu

Can you access my control via the www?
https://www.shodan.io/



entry
185.43.16.53
185-43-16-53.ip295.fastwebnet.it
Arpitel s.r.l.
Added on 2021-02-15 06:14:07 GMT
Italy, Foggia

```
HTTP/1.0 200 OK
Server: Phoenix-Contact/1.02 (powered by SpiderControl TM)
X-HitCounter: 397468
Connection: close
Content-Type: text/html
Content-Length: 3957
```

84.151.237.92
p5497ed5c.dip0.t-ipconnect.de
Deutsche Telekom AG
Added on 2021-02-15 09:32:37 GMT
Germany, Lemgo

```
HTTP/1.0 404 Not Found
Server: Phoenix-Contact/1.02 (powered by SpiderControl TM)
X-HitCounter: 40642
Cache-Control: no-cache
Pragma: no-cache
Expires: Mon, 01 Jan 1990 00:00:00 GMT
Connection: close
Content-Type: text/plain
```

SANS ICS Cyber Kill Chain

Adaptation / extension of the Cyber Kill Chain TM

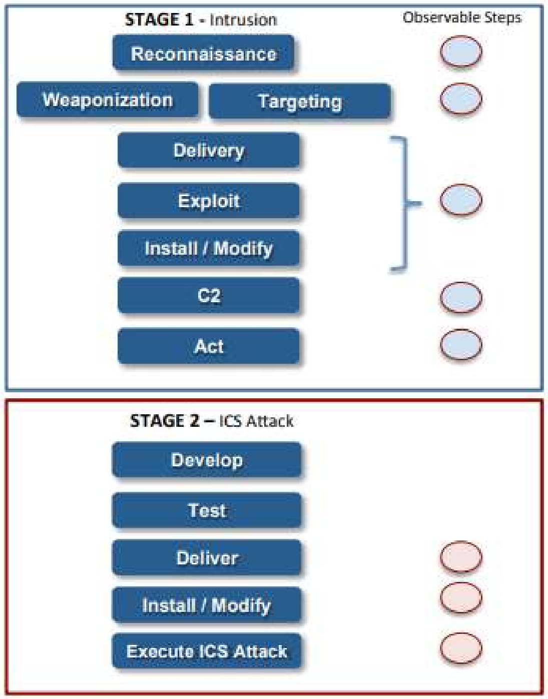
SANS Institute (SysAdmin, Networking, Security)

Two main stages

- Intrusion:

  Typically, an attack on classic IT, analogous to the Cyber Kill Chain TM
- ICS Attack:

  Targeted to OT / IACS systems and components, usually requiring in-depth knowledge of the target IACS environment



Source: SANS

Digital Factory | Data Security | Security evaluation

Effects of a security incident on automation systems

Production stops
What are the recovery costs?

Loss of know-how & sensitive data
Can the damage be quantified economically?

Blackmail with ransomware
What are the costs of reconstructing the data?

Loss of image
Is your reputation being questioned by partners and customers?

PHOENIX CONTACT
INSPIRING INNOVATIONS

DIGITAL FACTORY NOW

Digital Factory | Data Security | Security evaluation

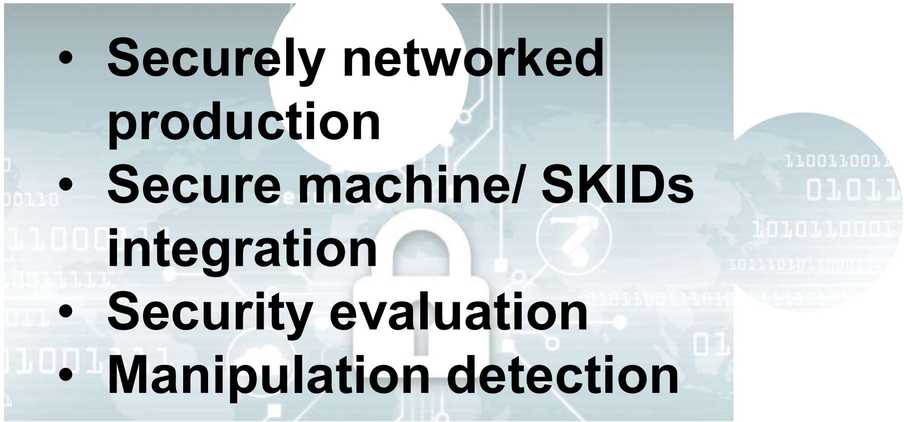
The Digital Factory toolbox

Data collection, storage & evaluation

Data transportation

Data security

Data usage



- **Securely networked production**
- **Secure machine/ SKIDs integration**
- **Security evaluation**
- **Manipulation detection**

Digital Factory | Data Security | Security evaluation

The differences between information (IT) and operation technology (OT)

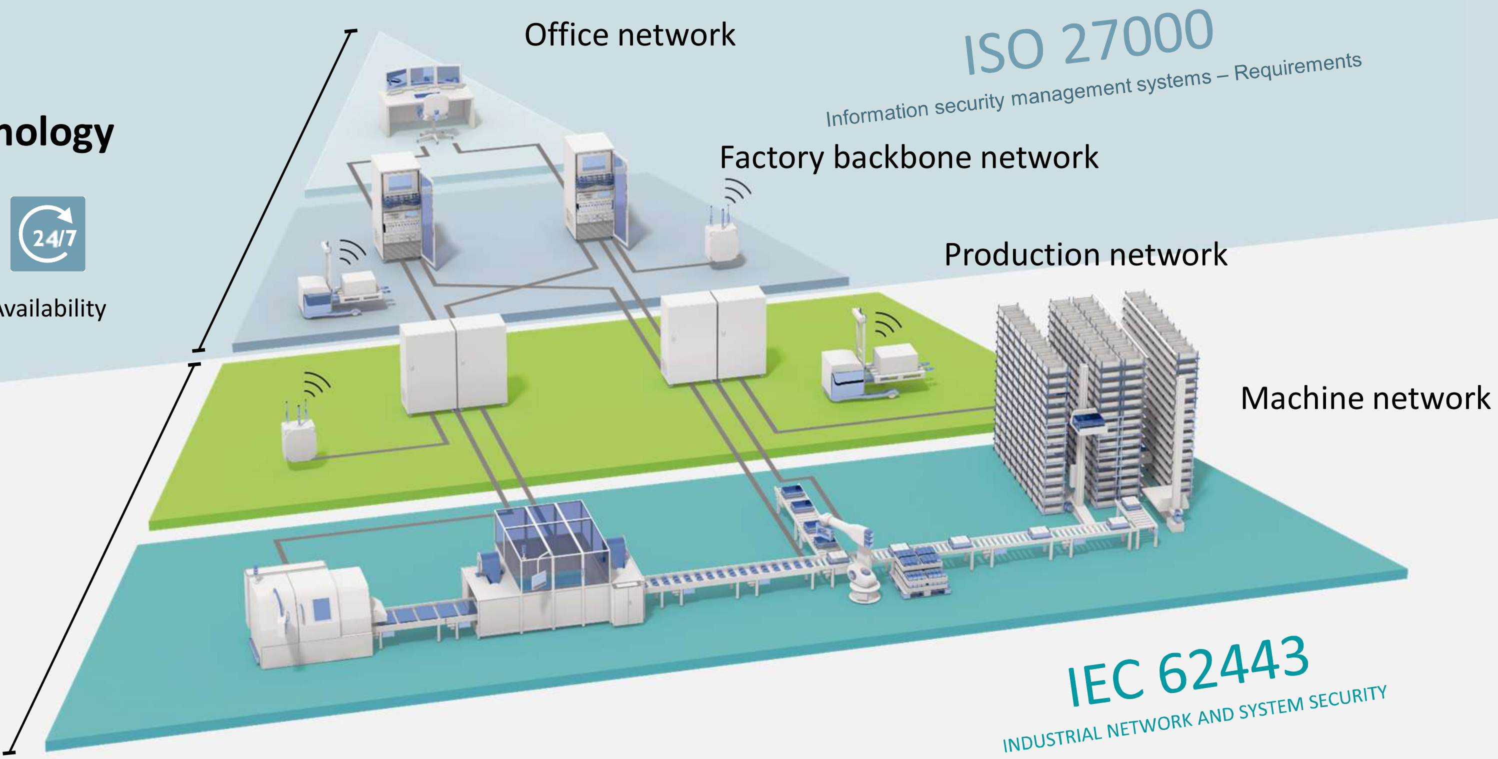
Information Technology

Confidentiality | Integrity | 24/7 Availability

≠

Operation Technology

24/7 Availability | Integrity | Confidentiality


Office network
ISO 27000
Information security management systems – Requirements
Factory backbone network
Production network
Machine network
IEC 62443
INDUSTRIAL NETWORK AND SYSTEM SECURITY

PHOENIX CONTACT
INSPIRING INNOVATIONS

ICS-Security[1] vs. IT-Security

Different priorities of the protection goals

ICS-Security

Avalibitity
Integrity
Confidentiality

IT-Security

Confidentiality
Integrity
Avalibitity

ICS-Security	Property	IT-Security
Failure cannot be tolerated	Availability	Short failure tolerable
Difficult	Reboot	Possible
Big challenge	Patch Management	Automated possible
7-20 years	Usage time	3-5 years

[1] **ICS Security** = **I**ndustrial **C**ontrol **S**ystems Security

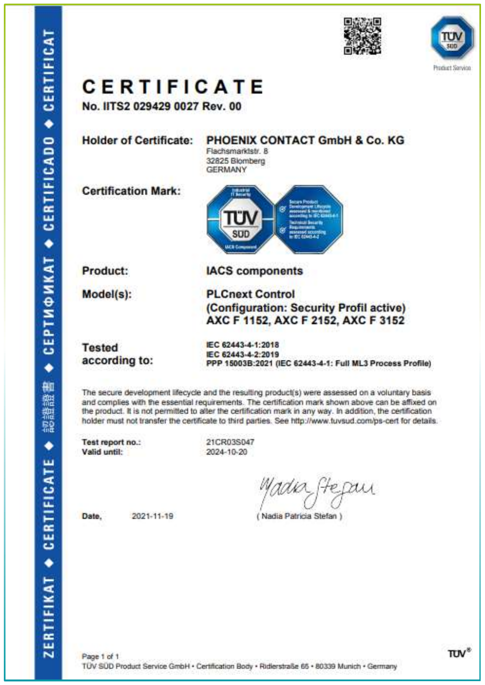
IIoT meets Security meets Functional Safety!

IoT
within an **IEC62443**
certified system!

Industrial
IT Security
TÜV
SÜD
IACS Component
Secure Product Development Lifecycle assessed & monitored according to IEC 62443-4-1
Technical Security Requirements assessed according to IEC 62443-4-2
RFC 4072S

- **PLCnext Control: AXC F 1152, 2152 and 3152**
- **PLC extension modul: AXC F XT SPLC 1000**
- **Safety Controller: RFC 4072S**

"The example of PLCnext Control shows how safety and security goals can be achieved in one product by cleverly dovetailing safety- and security-related tasks in the development process. Therefore, the product can be certified for both safety and security," adds Enrico Seidel, Senior OT-Security Expert at TÜV SÜD.


ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

TÜV SÜD
Product Service

CERTIFICATE
No. IITS2 029429 0027 Rev. 00

Holder of Certificate: **PHOENIX CONTACT GmbH & Co. KG**
Flachsmarktstr. 8
32825 Blomberg
GERMANY

Certification Mark:

Product: **IACS components**

Model(s): **PLCnext Control**
(Configuration: Security Profil active)
AXC F 1152, AXC F 2152, AXC F 3152

Tested according to: **IEC 62443-4-1:2018**
IEC 62443-4-2:2019
PPP 15003B:2021 (IEC 62443-4-1: Full ML3 Process Profile)

The secure development lifecycle and the resulting product(s) were assessed on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition, the certification holder must not transfer the certificate to third parties. See http://www.tuvsud.com/ps-cert for details.

Test report no.: 21CR03S047
Valid until: 2024-10-20

Date, 2021-11-19

Nadia Stefan
(Nadia Patricia Stefan)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany
TÜV®

Security evaluation

Plant shutdown

- What are the downtime and recovery costs?

Loss of know-how & sensitive data

- Can the damage be quantified economically?

Loss of image

- Is your reputation being questioned by partners and customers?

Blackmail with ransomware

- What are the costs of reconstructing the data?

Start now with the implementation of a holistic security concept according to IEC 62443 from Phoenix Contact.

Digital Factory | Data Security | Security evaluation

Security evaluation – Benefits for everyone

✓Secure your production against unauthorized access and cyber attacks

✓By creating a holistic concept in form of a blueprint you will learn more about industrial communication in your production

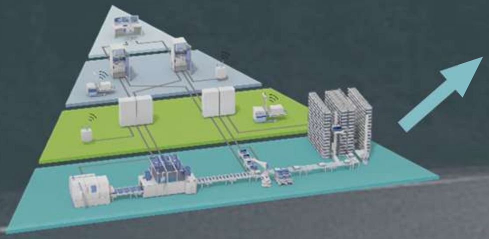
✓By Implementation and Verification of the concept you are not longer careless.

✓The blueprint can be used as a template for future production expansion

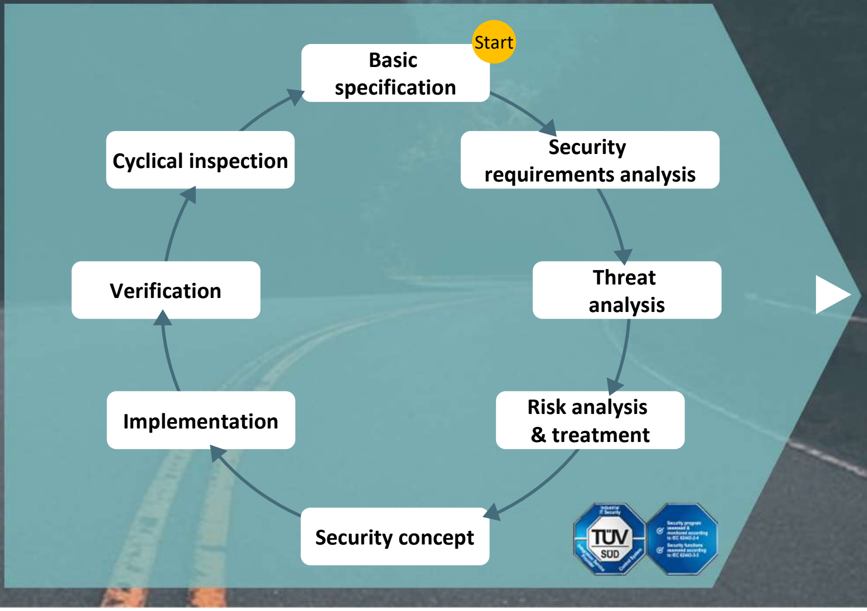
Digital Factory | Data Security | Security evaluation

Design of a security concept for automation solutions

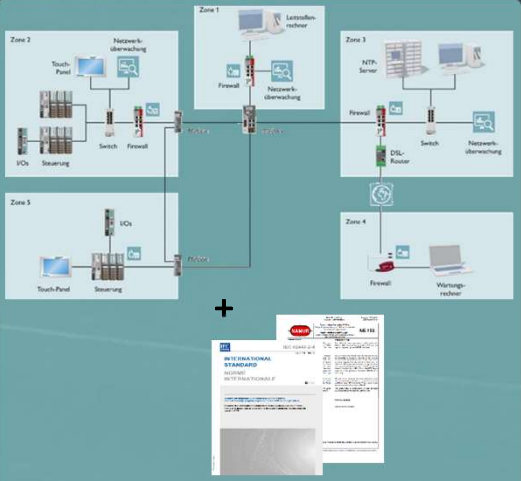
Starting point:
customer system information



Procedure:
Design of a security strategy for automation solutions



Result:
Holistic security strategy



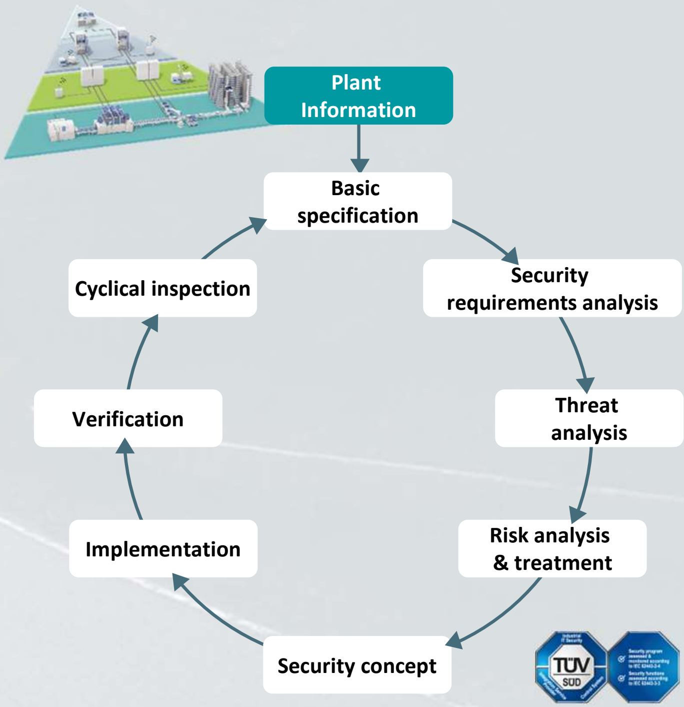
Security strategy with corresponding documentation of the individual process steps in accordance with IEC 62443

Digital Factory | Data Security | Security evaluation

The procedure in detail (1/9)

Activities

- Determination of the operational environment
- Determination of the assets with all the information necessary to create an asset list
- Definition of the network infrastructure
- Determination of the processes in the production plant.
- Definition of which information / data and communication relationships are worth protecting



Plant Information

Basic specification

Security requirements analysis

Threat analysis

Risk analysis & treatment

Security concept

Implementation

Verification

Cyclical inspection

PLCnext Technology

Designed by PHOENIX CONTACT

PLCnext Control

PLCnext Engineer

PLCnext Store

PLCnext Community

Brief overview

Competitive Advantages

PLCnext Control

OPC UA

Redundancy

Functional Safety

Edge Computing

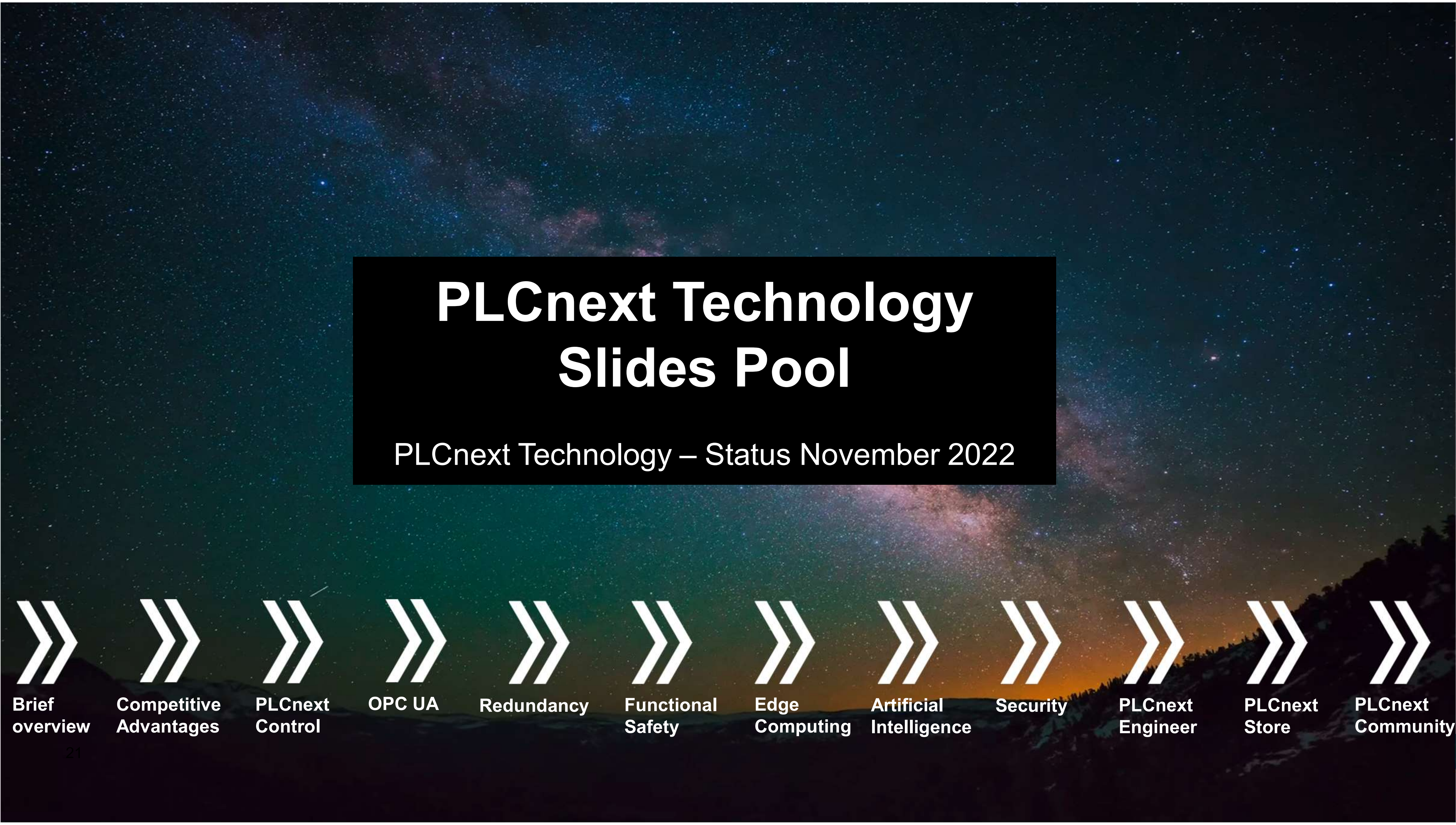
Artificial Intelligence

Security

PLCnext Engineer

PLCnext Store

PLCnext Community



PLCnext Technology Slides Pool

PLCnext Technology – Status November 2022

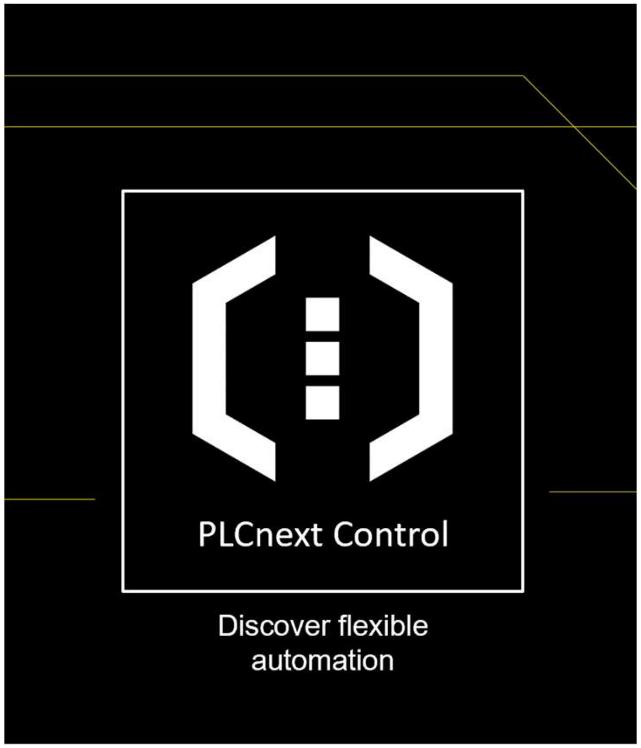
- Brief overview
- Competitive Advantages
- PLCnext Control
- OPC UA
- Redundancy
- Functional Safety
- Edge Computing
- Artificial Intelligence
- Security
- PLCnext Engineer
- PLCnext Store
- PLCnext Community

PLCnext Technology

The open ecosystem for limitless automation

Safety

with PLCnext Control



PLCnext Control

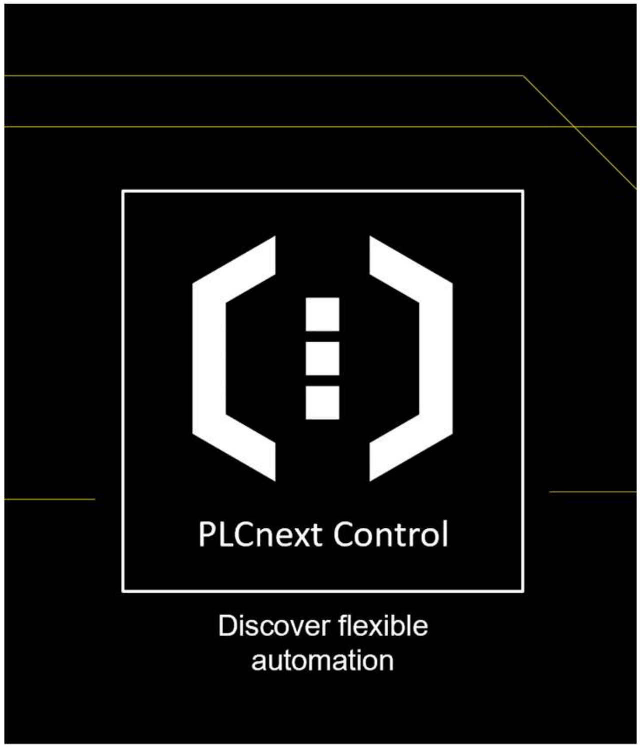
Discover flexible automation

PLCnext Technology

The open ecosystem for limitless automation

Safety

with PLCnext Control



PLCnext Control

Discover flexible automation

PLCnext Control Extension SPLC 1000

PLCnext Extension AXC F XT SPLC 1000

Core	# of Profisafe devices	Temperature
2 x Cortex M4	32	-25°C - 60°C
Width	**Approvals**	**C Functions**
45mm	UL, CUL, etc	Reloadable

PLCnext Technology

PLCnext Control RFC 4072S

Core

Intel i5 6300U 2 x 2,4 GHz processor

Random Access Memory

4 GB DDR 4 dual channel RAM

Temperature

0°C up to 55°C with fan

# control tasks (IEC 61131)

32

Min. cycle time (IEC 61131)

0,5 ms

Security

TPM integrated

PLCnext Technology

PLCnext Control BPC 9102S

Core	Random Access Memory	Temperature
Octa-Core Intel Core i7-10700TE	**16 GB DDR 4 RAM**	**-20°C up to 60°C**
# control tasks (IEC 61131)	Min. cycle time (IEC 61131)	Security
128	**0,5 ms**	**TPM integrated**

PLCnext Control

PLCnext Safety Extension AXC F XT SPLC 1000

- Scalable PLCnext Safety Control
- Reloadable C-Functions, e.g.
  - Complex safety algorithm
  - Safety Machine Learning
  - Automatic certification
- Adaptable Safety Communication, e.g.
  - OPC UA Safety (M2M)
  - PROFIsafe (M2D)
  - Vendor specific
- Approvals
  - SIL3, PLe
  - UL (Hazloc), CUL
  - IEC Ex, ATEX

PLCnext Control Extension
AXC F XT SPLC 1000
Safety
RUN
FS
Ord. No. 1159811
Ord.No. 2404267 AXC F 2152
SD-CARD
PLCnext Technology
BF-C
BF-D
SF
BOOT
EXT
RUN
FAIL
DBG
D
E
scan here for easy start up
www.plcnext-community.net

- Scalable PLCnext Control
- Open ecosystem for limitless automation
- IEC 61131-3, C, C++, C#, Matlab
- OPC UA, MQTT, ...
- Open communication standards
- Security by design
- Built-in cloud connectivity

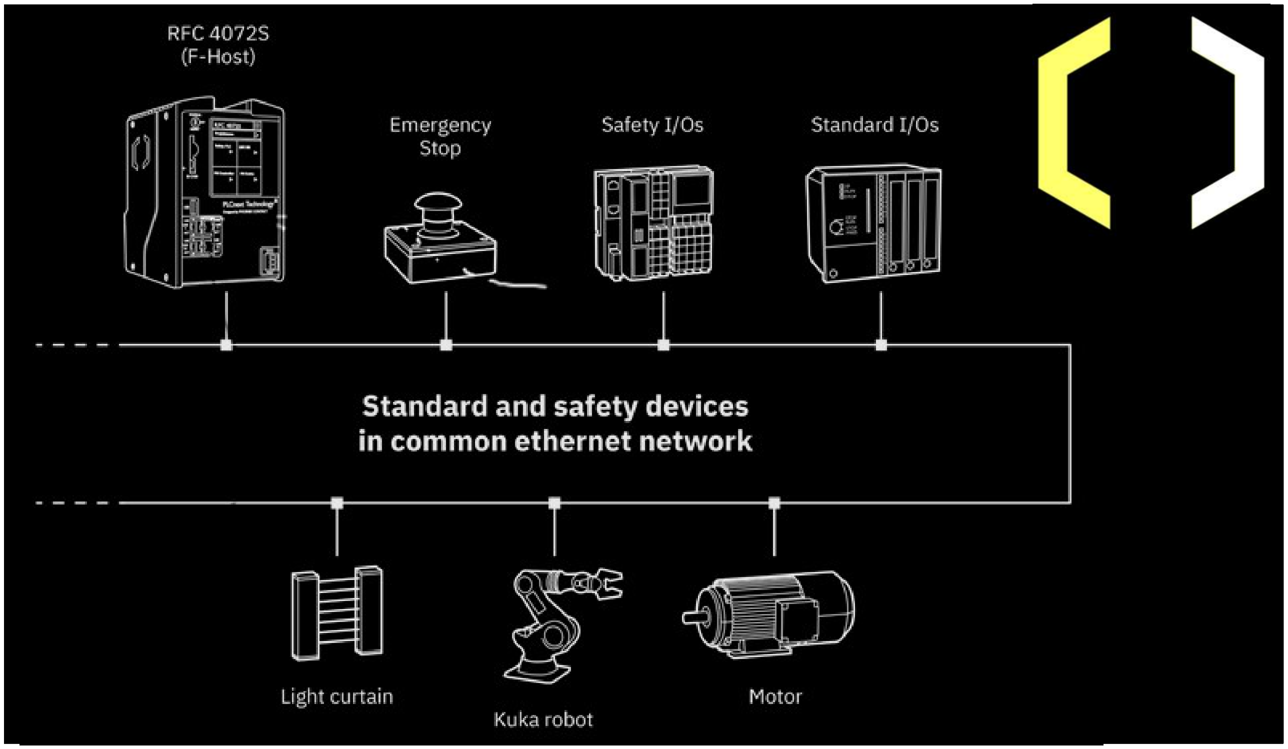
PLCnext Technology - Scalable Safety PLC

AXC F XT SPLC 1000 – Modular Safety PLC

- Decentralized Small Safe PLC
- Connectable to PLCnext Controls as extension Modul
- Supported Safety Protocols:
  - PROFIsafe V2.61 (32 instances)
- Connectable to higher-layer SPLC as F-Device and via new OPC UA Safety Protocol

PLCnext Technology
Designed by PHOENIX CONTACT

Safety and Standard communication in one Network

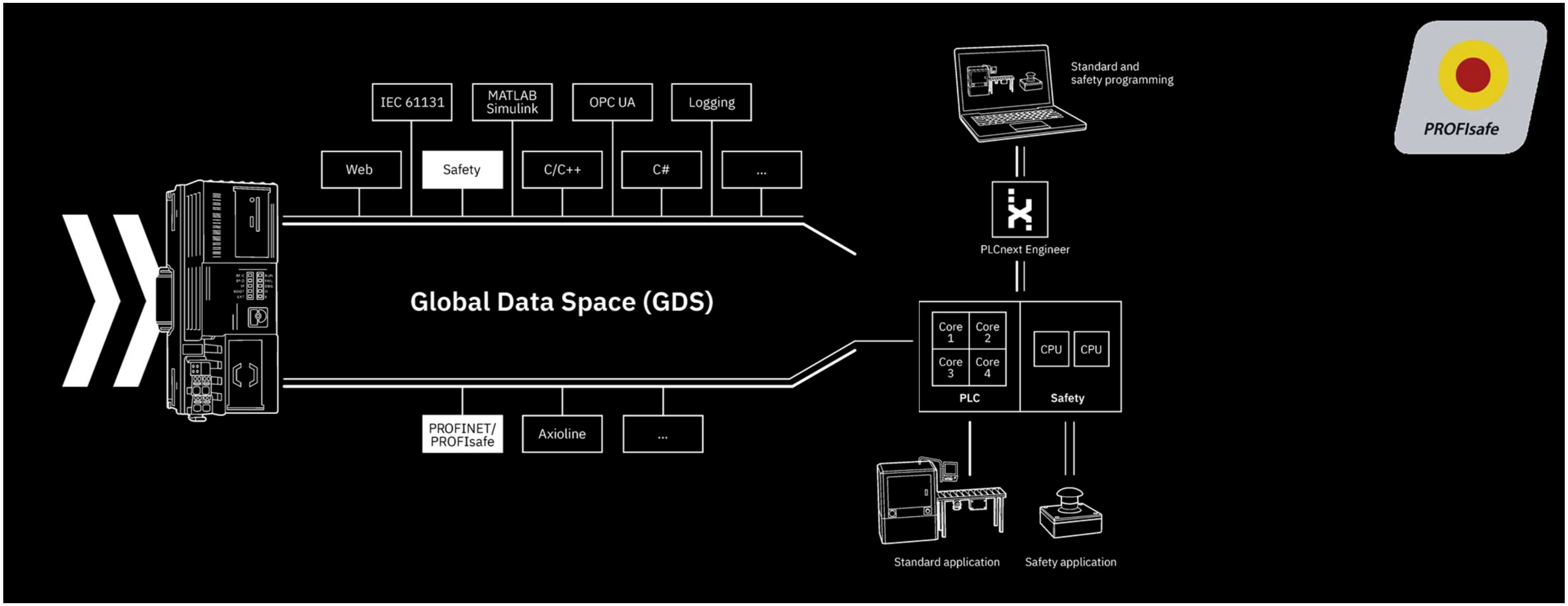


Fully integrated Safety programming

- TÜV Rheinland certified according to IEC 61508
- Editor with common behavior as known from standard FBD or LD editors
- Low Variability Language support
- Networkt granular CRC checksums
- PROFIsafe Support

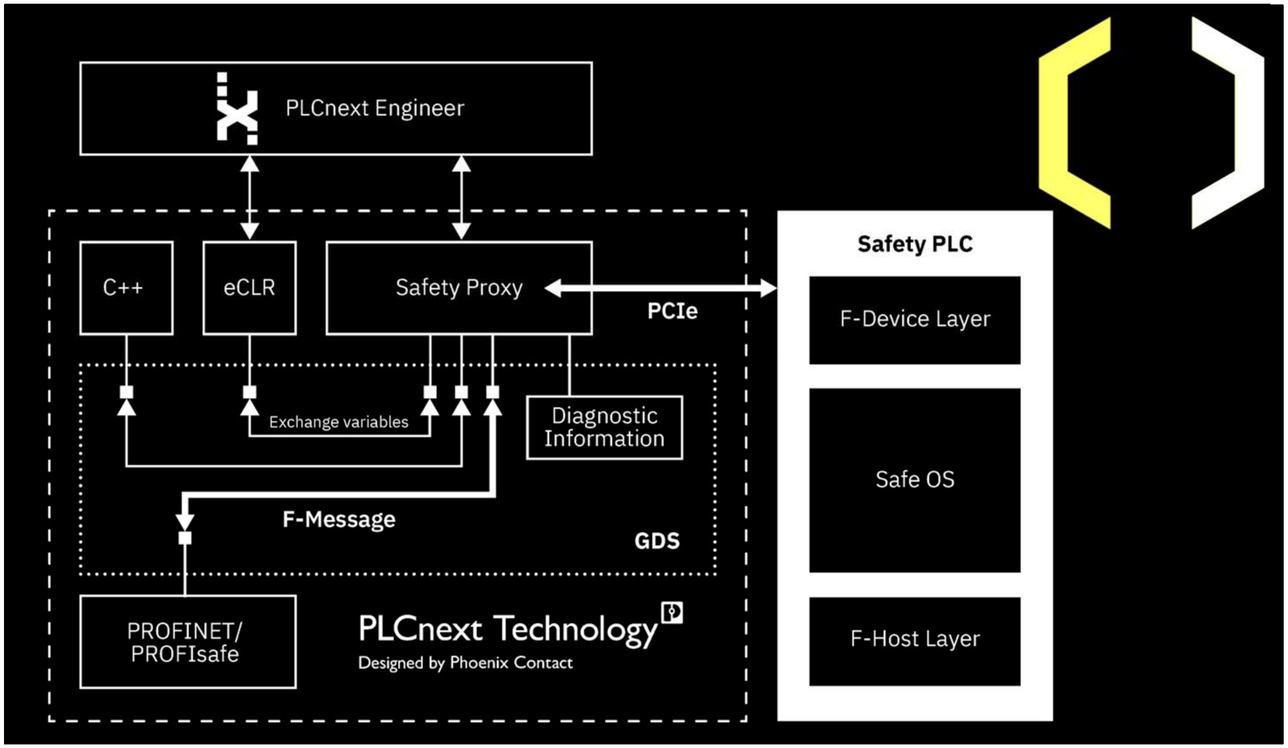
PLCnext Technology Components

Safety integrated



Functional Safety Integration

Safety Integrated



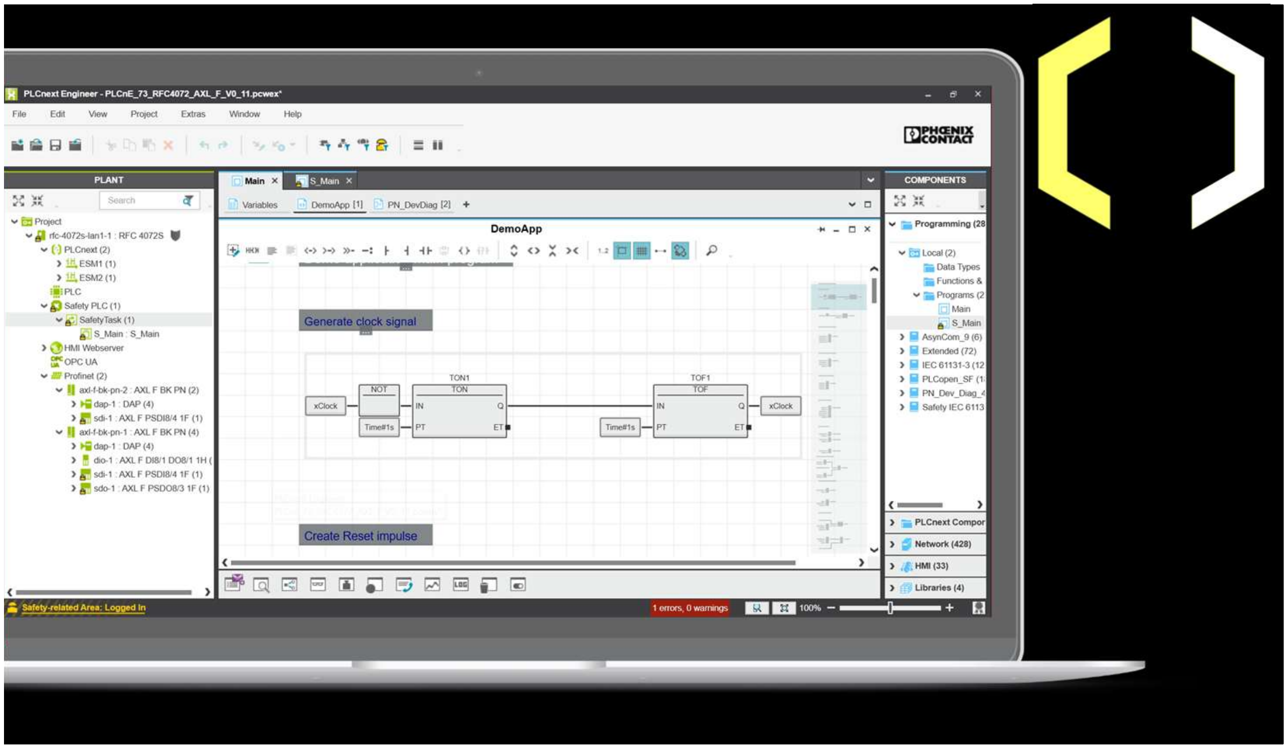
Fully integrated Safety

- Safety integrated (programming, hardware configuration)
- Consistent usability
- SIL 3 / PL e
- Separate Safety PLC
    - 2 channel architecture
- Profisafe Host/ / Device integrated

PLCnext Technology
Designed by PHOENIX CONTACT

Standard and safety programming in one engineering software

PLCnext Engineer



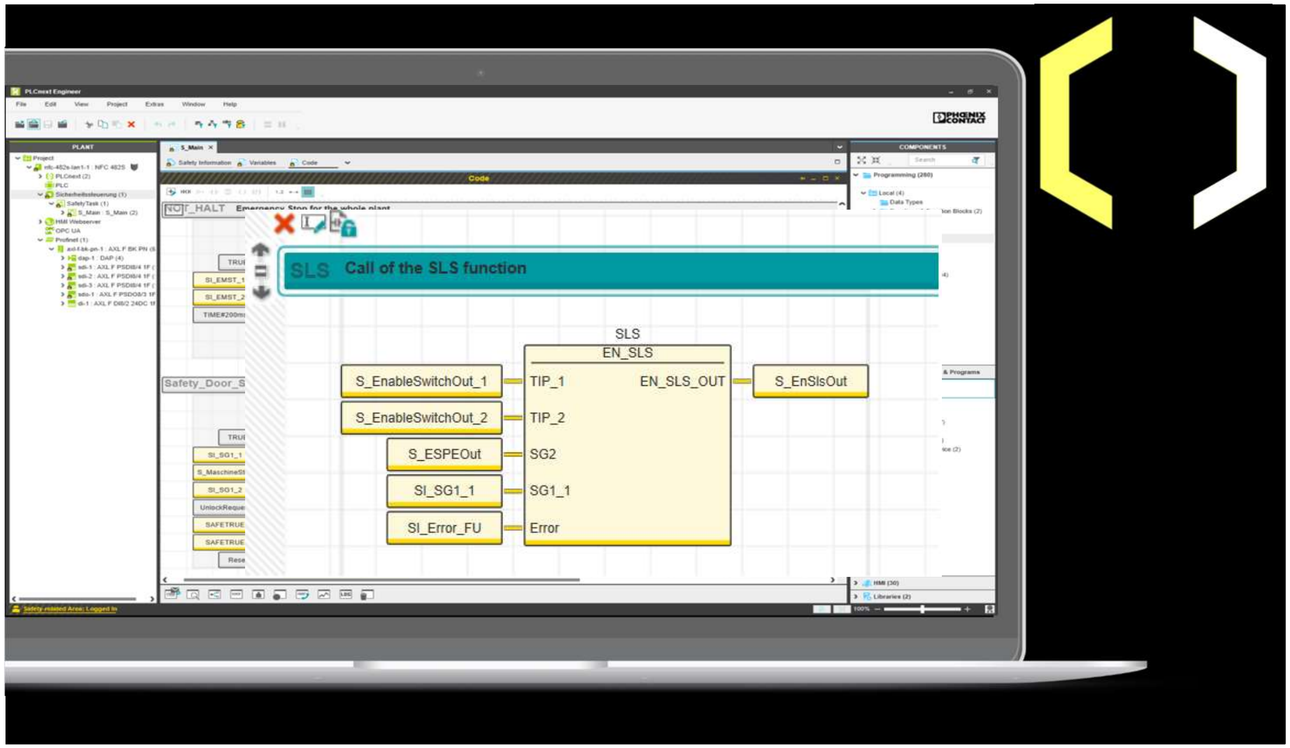
Fully integrated Safety programming

- TÜV Rheinland certified according to IEC 61508
- Editor with common behavior as known from standard FBD or LD editors
- Low Variability Language support
- Networkt granular CRC checksums
- PROFIsafe Support

PHOENIX CONTACT
INSPIRING INNOVATIONS

Standard and safety programming in one engineering software

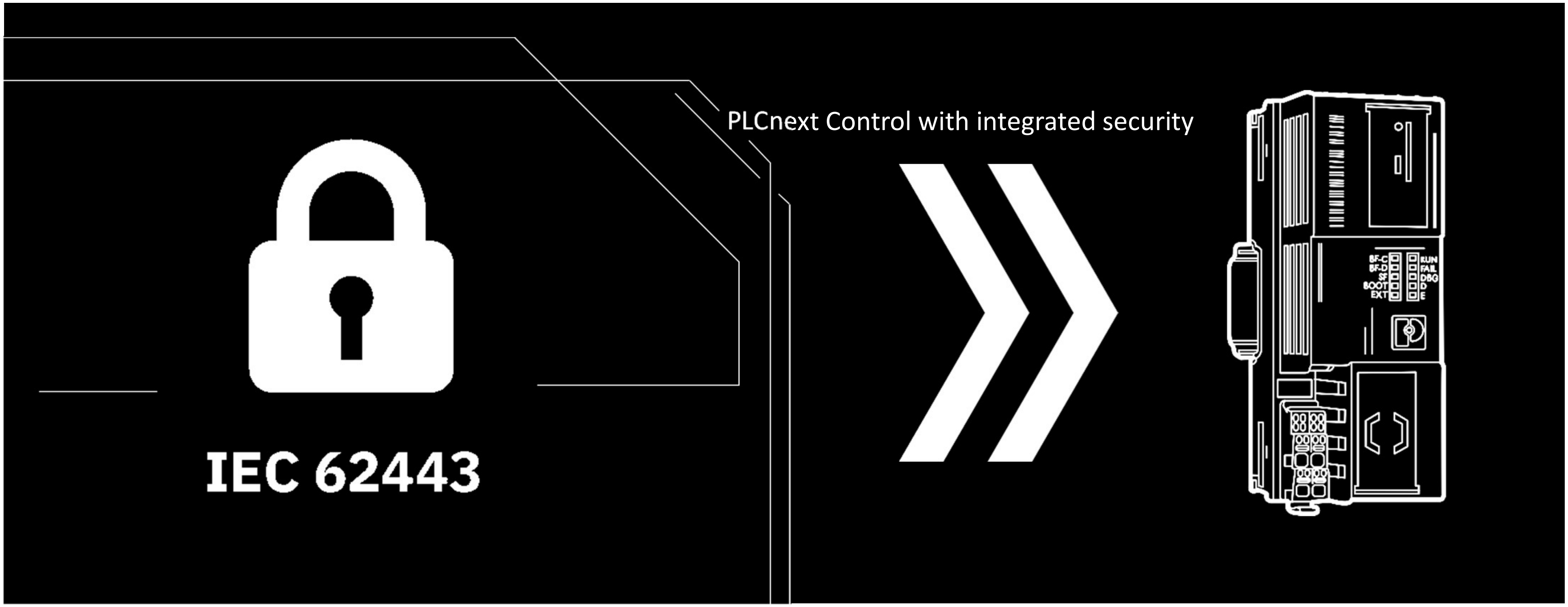
PLCnext Engineer



Fully integrated Safety programming

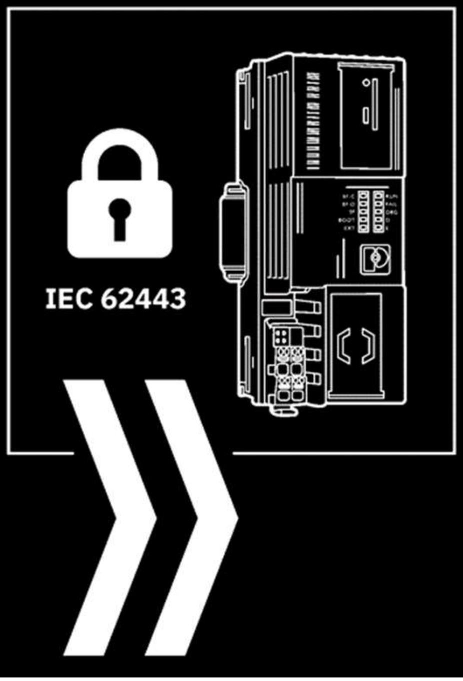
- Individual safety functions can be protected by a verification function
- Background signal path analysis
- Background safe semantic analysis
- Diversely-redundant code generator

PLCnext Control according to the standard IEC 62443



IEC 62443 - Security for Industrial Automation & Control Systems

Effects of Security Incidents on Production Facilities



Plant downtime

Due to security problems, production has to be stopped for hours or days. What are the costs of such a production downtime?

Loss of know-how

A competitor can access your sensitive data (design, engineering,…). Can you quantify the damage economically?

Data loss

Suddenly all data is lost. What would be the cost of reconstructing this data?

Standing

What happens if your reputation for the reliability and security of your company’s data is compromised by your partners?

Applicable Security Laws and Standards

Brief Overview of the Most Important Laws & Standards

Security Laws (What must be done?)

Bundesministerium des Innern

Version 2.0 in preparation

IT Security Act (2015)

Asset owner of critical infrastructures must establish and certificate an **ISMS** (**I**nformation **S**ecurity **M**anagement **S**ystem) as well as fulfill a set of minimum technical requirements

EU Cybersecurity Act (3/2019)

A comprehensive set of regulations, technical requirements, standards and procedures for certification or conformity assessment of products

Recommendations (What should be done?)

Bundesamt für Sicherheit in der Informationstechnik

BSI IT Basic Protection Catalogs
(asset owner / device manufacturer)

Basic Security Standards (How to implement?)

IEC 62443 Security for industrial automation
(asset owner / device manufacturer)

ISO/IEC 2700X Information Technology
(asset owner)

Applicable Security Laws and Standards

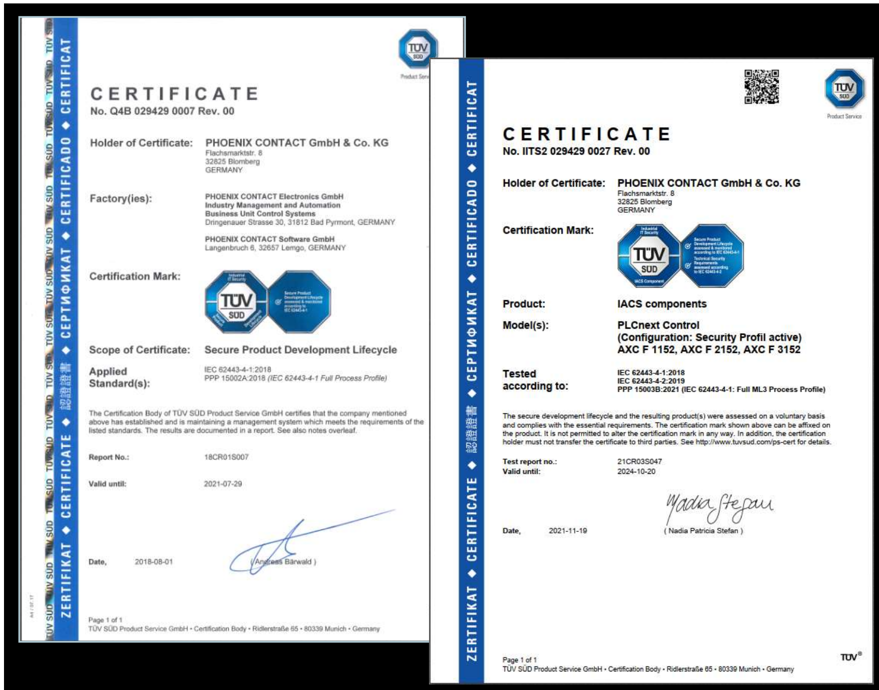
Sector-specific Security Standards

Standard	Target Group	Main Purpose	Geographical / Industry Focus	Certification possible?
BDEW	Device manufacturers / system integrators	Security requirements for suppliers	D, A, CH Energy & water sectors	No
WIB	Device manufacturers / system integrators	Device manufacturer certification	Oil & Gas sector	Yes
ISO/IEC 27019	Asset owners / plant operators	IT security for control systems	Energy sector	Yes
NIST 800-82	Asset owners / plant operators	Technical security recommendations	USA	No
NERC CIP	Asset owners / plant operators	Increasing reliability of energy supply infrastructure	USA, Canada	Yes
IEC 62443	Device manufacturers / system integrators / plant operators	Requirements for secure products, secure solutions, and secure operation	General industry sector	Yes

PLCnext Technology – Security

PLCnext Technology
Designed by PHOENIX CONTACT

IEC 62443: IT-Security for Industrial Automation Control Systems



CERTIFICATE
No. Q4B 029429 0007 Rev. 00

Holder of Certificate: **PHOENIX CONTACT GmbH & Co. KG**
Flachsmarktstr. 8
32825 Blomberg
GERMANY

Factory(ies): **PHOENIX CONTACT Electronics GmbH**
Industry Management and Automation
Business Unit Control Systems
Dringenauer Strasse 30, 31812 Bad Pyrmont, GERMANY

PHOENIX CONTACT Software GmbH
Langenbruch 6, 32657 Lemgo, GERMANY

Certification Mark:

Scope of Certificate: **Secure Product Development Lifecycle**

Applied Standard(s): IEC 62443-4-1:2018
PPP 15002A:2018 *(IEC 62443-4-1 Full Process Profile)*

The Certification Body of TÜV SÜD Product Service GmbH certifies that the company mentioned above has established and is maintaining a management system which meets the requirements of the listed standards. The results are documented in a report. See also notes overleaf.

Report No.: 18CR01S007

Valid until: 2021-07-29

Date, 2018-08-01

(Andreas Bärwald)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

CERTIFICATE
No. IITS2 029429 0027 Rev. 00

Holder of Certificate: **PHOENIX CONTACT GmbH & Co. KG**
Flachsmarktstr. 8
32825 Blomberg
GERMANY

Certification Mark:

Product: **IACS components**

Model(s): **PLCnext Control**
(Configuration: Security Profil active)
AXC F 1152, AXC F 2152, AXC F 3152

Tested according to: **IEC 62443-4-1:2018**
IEC 62443-4-2:2019
PPP 15003B:2021 (IEC 62443-4-1: Full ML3 Process Profile)

The secure development lifecycle and the resulting product(s) were assessed on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition, the certification holder must not transfer the certificate to third parties. See http://www.tuvsud.com/ps-cert for details.

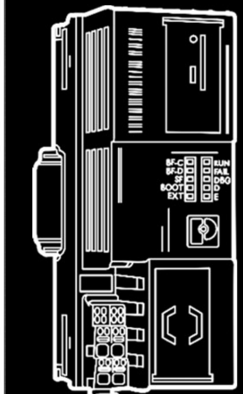
Test report no.: 21CR03S047
Valid until: 2024-10-20

Nadia Stefan

Date, 2021-11-19 (Nadia Patricia Stefan)

Page 1 of 1
TÜV SÜD Product Service GmbH • Certification Body • Ridlerstraße 65 • 80339 Munich • Germany

ZERTIFIKAT ◆ CERTIFICATE ◆ 認證證書 ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT
TÜV SÜD
Product Service
TÜV®


BF-C
BF-D
SF
BOOT
EXT
RUN
FAIL
DBG
D
E

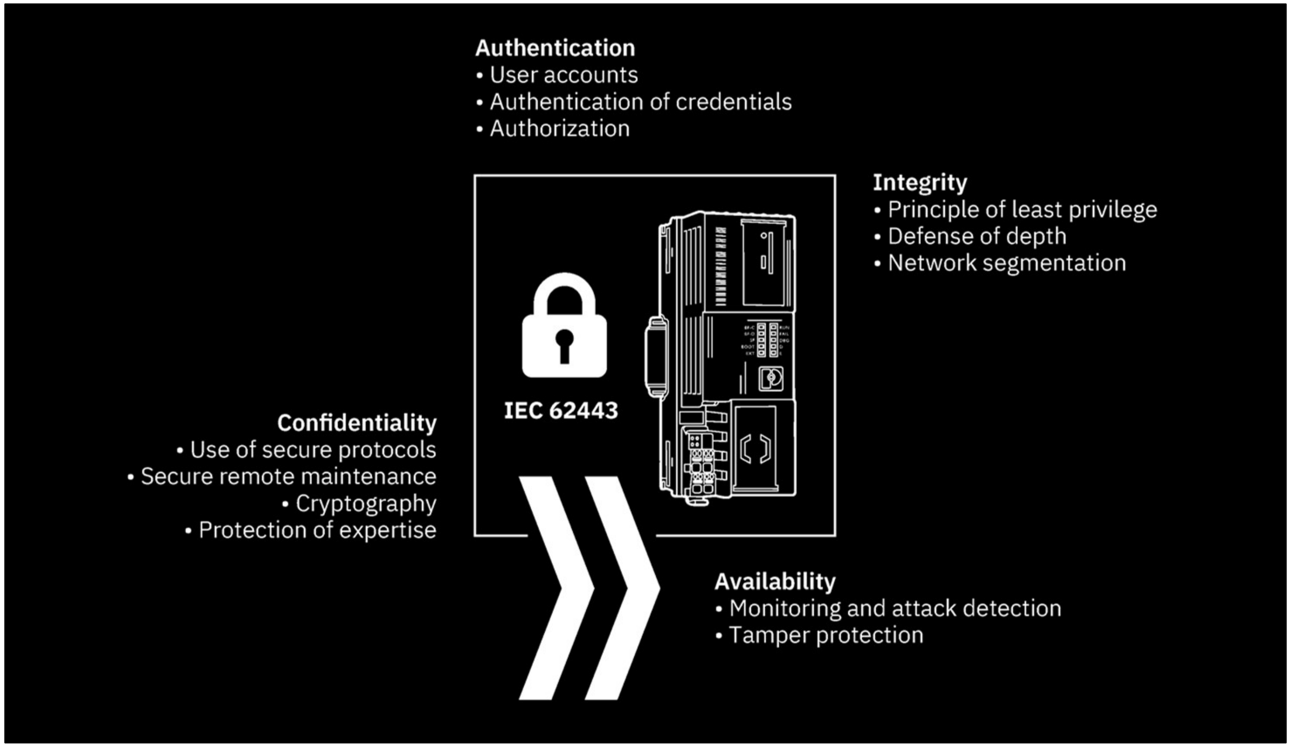
IEC 62443

Industrial Automation Basis Standard

PHOENIX CONTACT
INSPIRING INNOVATIONS

Applicable Security Laws and Standards

IEC 62443: IT-Security for Industrial Automation Control Systems



Authentication
- User accounts
- Authentication of credentials
- Authorization

Integrity
- Principle of least privilege
- Defense of depth
- Network segmentation

Confidentiality
- Use of secure protocols
- Secure remote maintenance
- Cryptography
- Protection of expertise

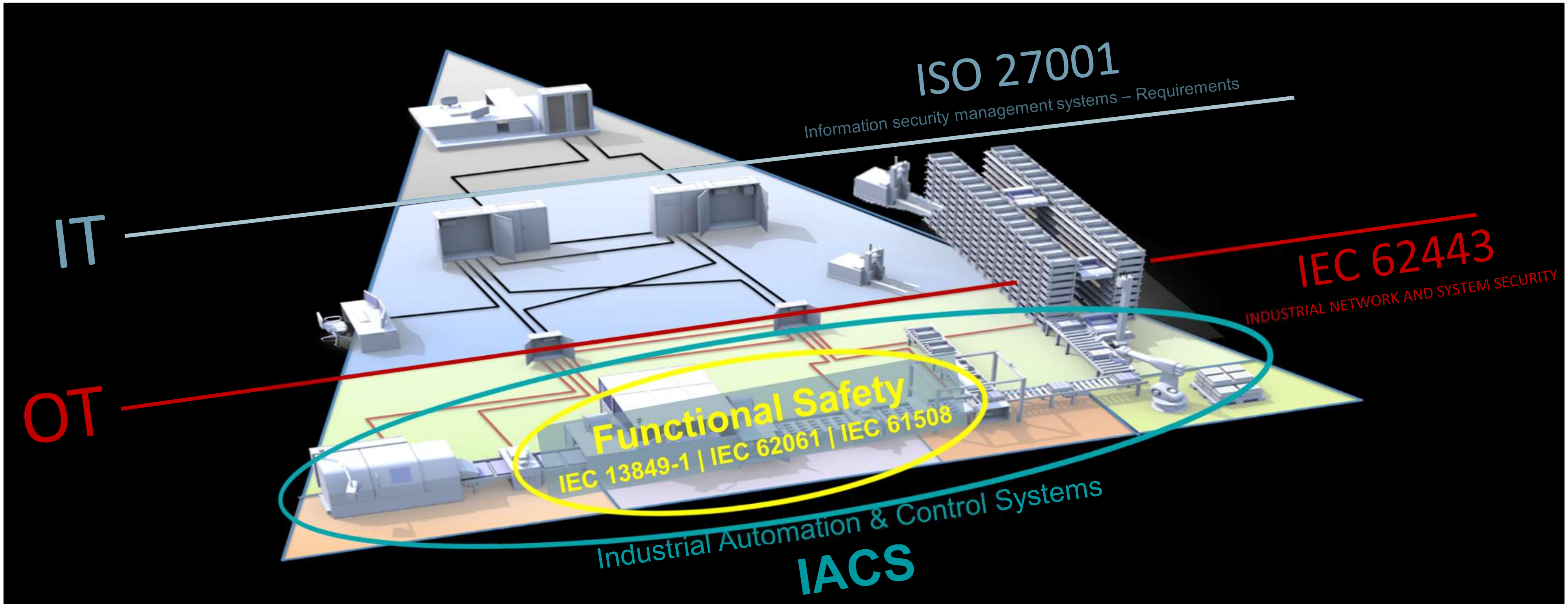
Availability
- Monitoring and attack detection
- Tamper protection

IEC 62443

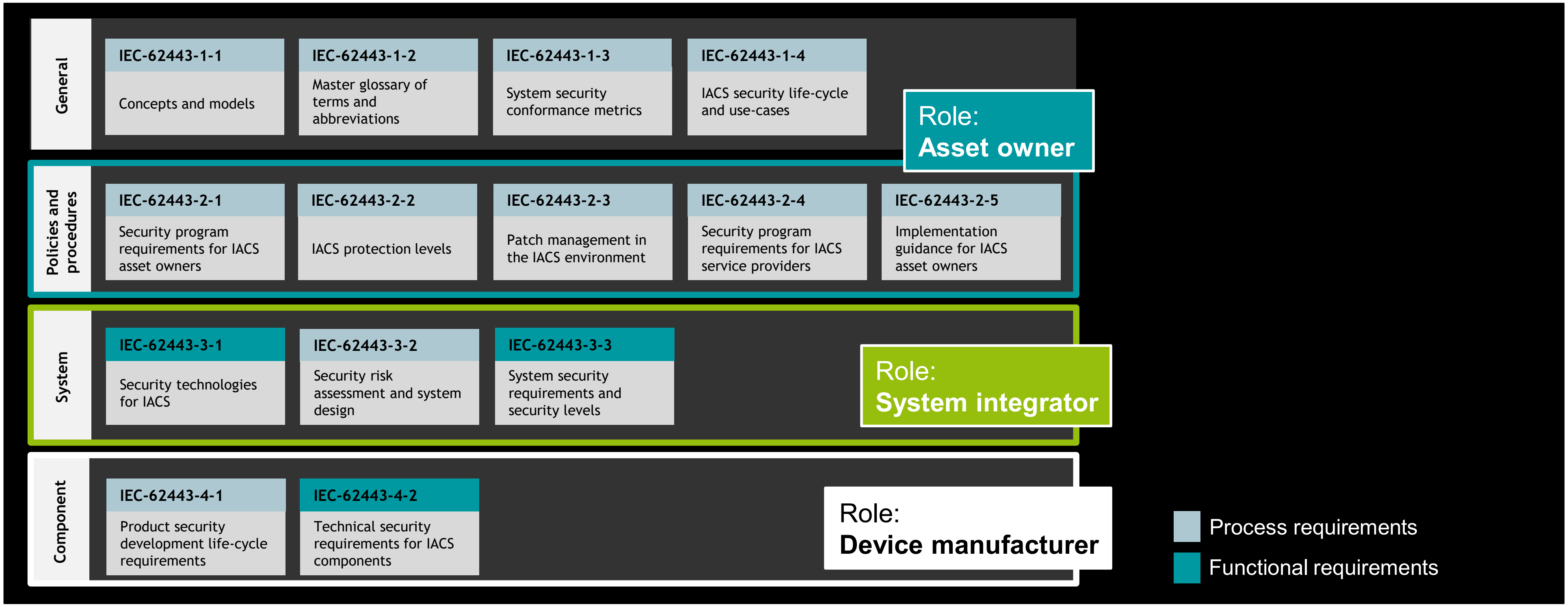
Industrial Automation Basis Standard

Terminology, Roles, and Tasks in Security Processes

The "Automation Pyramid"


ISO 27001
Information security management systems – Requirements
IT
IEC 62443
INDUSTRIAL NETWORK AND SYSTEM SECURITY
OT
Functional Safety
IEC 13849-1 | IEC 62061 | IEC 61508
Industrial Automation & Control Systems
IACS

IEC 62443 Structure and Systematics



General	IEC-62443-1-1 Concepts and models	IEC-62443-1-2 Master glossary of terms and abbreviations	IEC-62443-1-3 System security conformance metrics	IEC-62443-1-4 IACS security life-cycle and use-cases	
Policies and procedures	IEC-62443-2-1 Security program requirements for IACS asset owners	IEC-62443-2-2 IACS protection levels	IEC-62443-2-3 Patch management in the IACS environment	IEC-62443-2-4 Security program requirements for IACS service providers	IEC-62443-2-5 Implementation guidance for IACS asset owners
System	IEC-62443-3-1 Security technologies for IACS	IEC-62443-3-2 Security risk assessment and system design	IEC-62443-3-3 System security requirements and security levels		
Component	IEC-62443-4-1 Product security development life-cycle requirements	IEC-62443-4-2 Technical security requirements for IACS components			

Role:
Asset owner

Role:
System integrator

Role:
Device manufacturer

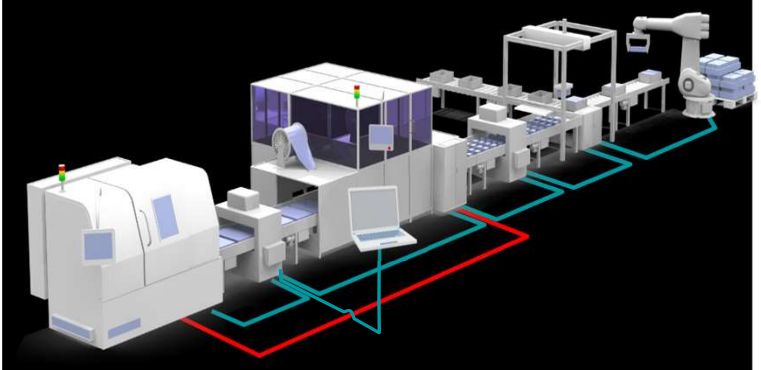
▨ Process requirements

■ Functional requirements

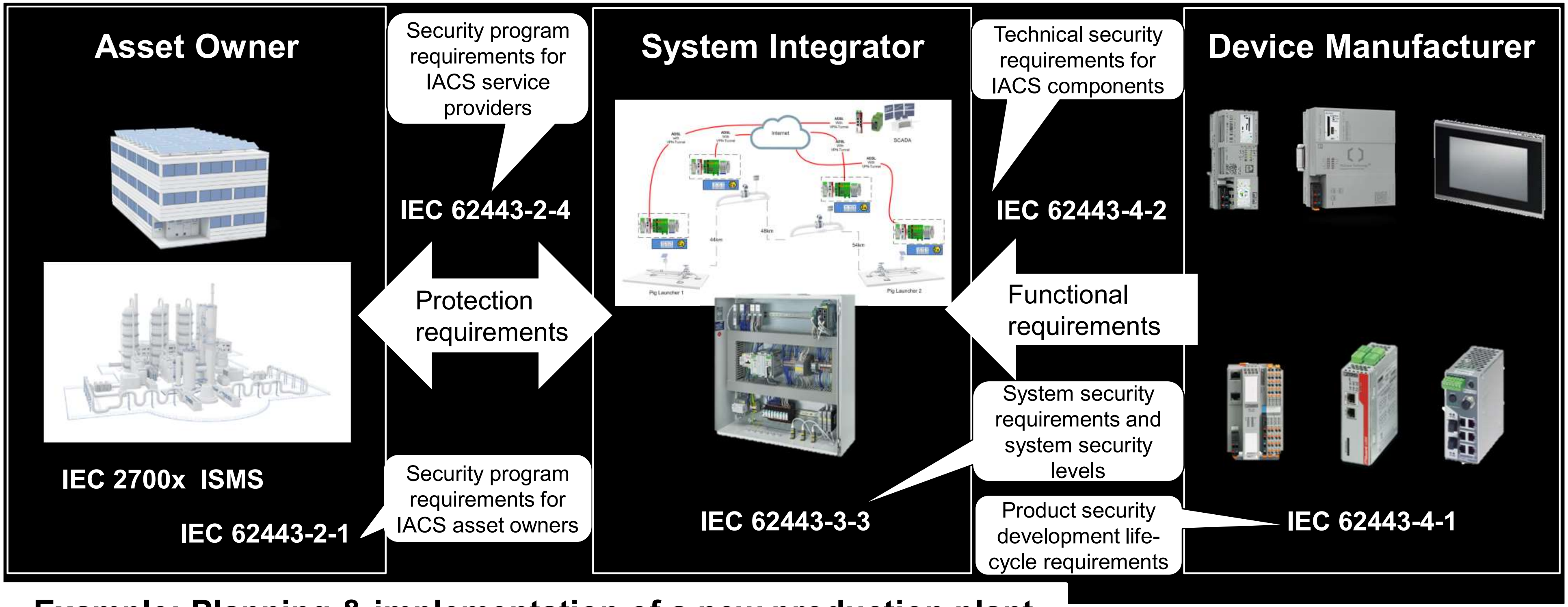
Basic Roles & Purposes of the IEC 62443 Standard

Role	Focus	Interest
Asset owner / plant operator	Operation & maintenance of automation solutions	Secure operation
System integrator / Machine builder	Design & commissioning of automation solutions	Secure solution
Device manufacturer	Design & management of components for automation solutions	Secure devices

Companies can check their automation technology for potential weaknesses and develop protective measures



Role Distribution in a Value-added Chain according to IEC 62443



Asset Owner

IEC 2700x ISMS

IEC 62443-2-1

Security program requirements for IACS asset owners

Security program requirements for IACS service providers

IEC 62443-2-4

Protection requirements

System Integrator

IEC 62443-3-3

System security requirements and system security levels

Technical security requirements for IACS components

IEC 62443-4-2

Functional requirements

Product security development life-cycle requirements

Device Manufacturer

IEC 62443-4-1

Example: Planning & implementation of a new production plant

Secure Product Development

IEC 62443-3-3: Security Level Def

Functional requirements				
Attacker capabilities				
Security Level	Means	Resources		
SL - 0	no protection requirements			
SL - 1	casual or coincidental manipulatio			
SL - 2	simple	low		
SL - 3	sophisticated	moderate	IACS specific	moderate
SL - 4	sophisticated	extended	IACS specific	high

Protection against the abilities of…

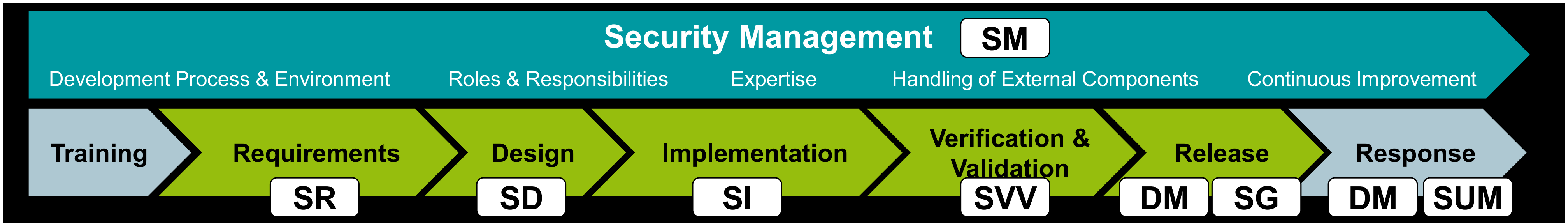
SL-1
…any Internet user

SL-2
… interested individuals and companies with generic security knowledge

SL-3
… experts and companies that develop and deploy effective, yet cost-oriented attack scenarios with clear goals

SL-4
… governmental organizations which focus on achieving the specifically selected target at almost any price

IEC 62443-4-1: Product Development & Lifecycle

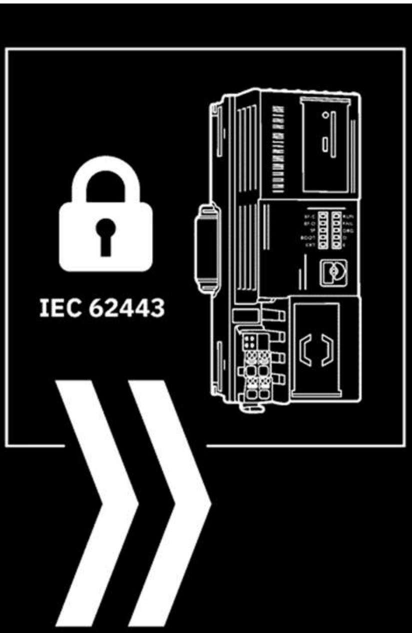


1. **SM** Security Management
2. **SR** Security Requirements
3. **SD** Secure by Design
4. **SI** Secure Implementation
5. **SV** Security Verification and Validation testing
6. **DM** Security Defect Management
7. **SUM** Security Update Management
8. **SG** Security Guidelines

IEC 62443 4-1 defines
8 practices & 47 requirements

PLCnext Technology Security by Design

Security Features Summary



Home (plcnext.help)

- Security Architecture: Configurable Linux based on Yocto Build System
- Hardware design with: TPM -> IEEE 802.1 AR (Secure Device Identity)
- Network segmentation for Zones and Conduits management AXC F XT ETH 1TX Extension module integrated in the firewall
- Integrity check during boot process
- Secure Communication: TLS, SFTP, VPN, HTTPS, …..
- User Management with enhanced complexity rules and central AD (LDAP)
- Linux nftables Firewall with netload limiter
- VPN IPSec IKEv1/2 Strongswan and Open VPN file configuration
- SYSLOG for security message management and central storage on server
- OPC UA security signed & encrypted with certificate management via GDS
- SD card activation / deactivation / encryption
- Device and Patch Management / OPC UA FW Update

Digital Factory | Data transportation | Smart automation network

Network products

FL Switch 2000

Managed switches

- Gigabit and fibre optic
- Redundancy protocols
- Diagnostic features
- Security functions
- Usability

FL Network Manager

Software

- Scan existing network
- Device configuration
- Firmware update
- Graphic topology overview

Optional: FL MGUARD

Security

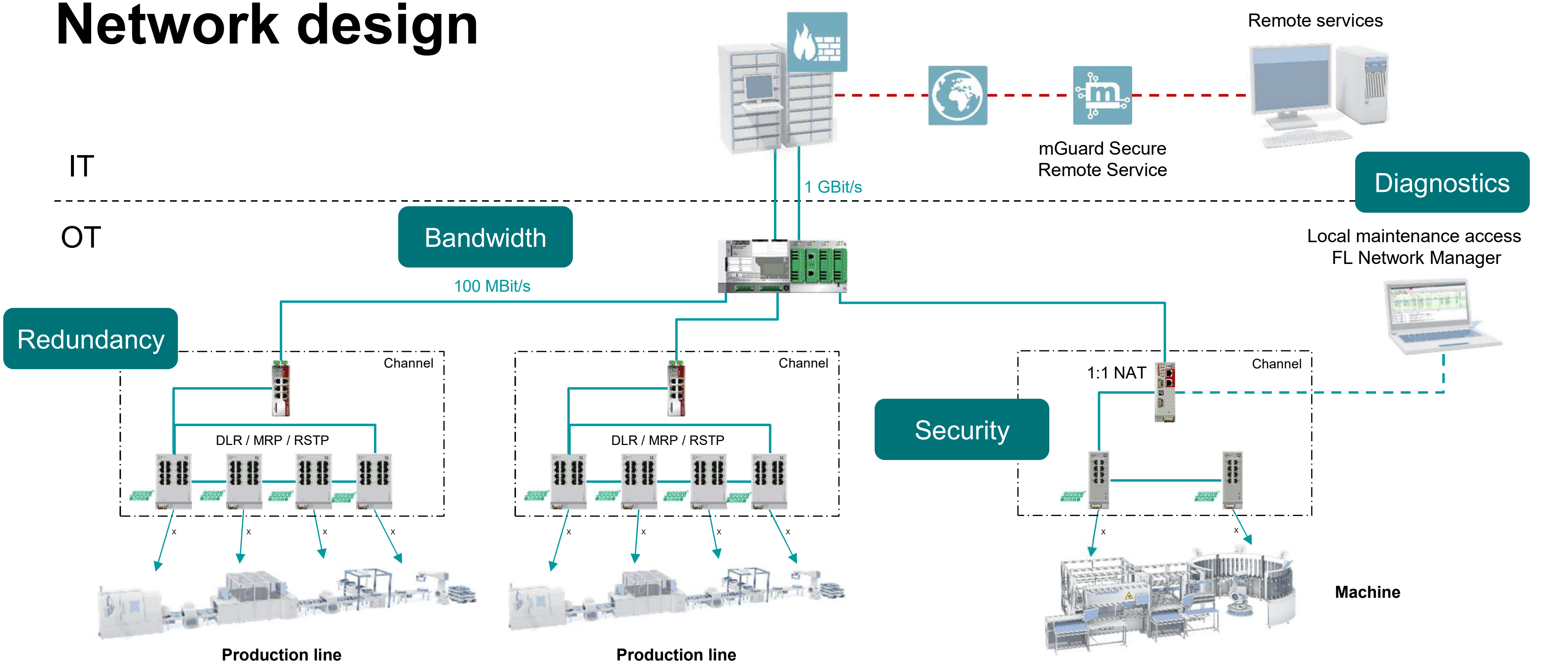
- Hardware based protection
- VPN router
- NAT routing
- Integrity monitoring of windows file system

Digital Factory | Data transportation | Smart automation network

Network design

🟦 Ethernet

🟥 VPN connection



Remote services

mGuard Secure Remote Service

Diagnostics

IT

OT

1 GBit/s

Bandwidth

100 MBit/s

Local maintenance access FL Network Manager

Redundancy

Security

Channel

Channel

Channel

1:1 NAT

DLR / MRP / RSTP

DLR / MRP / RSTP

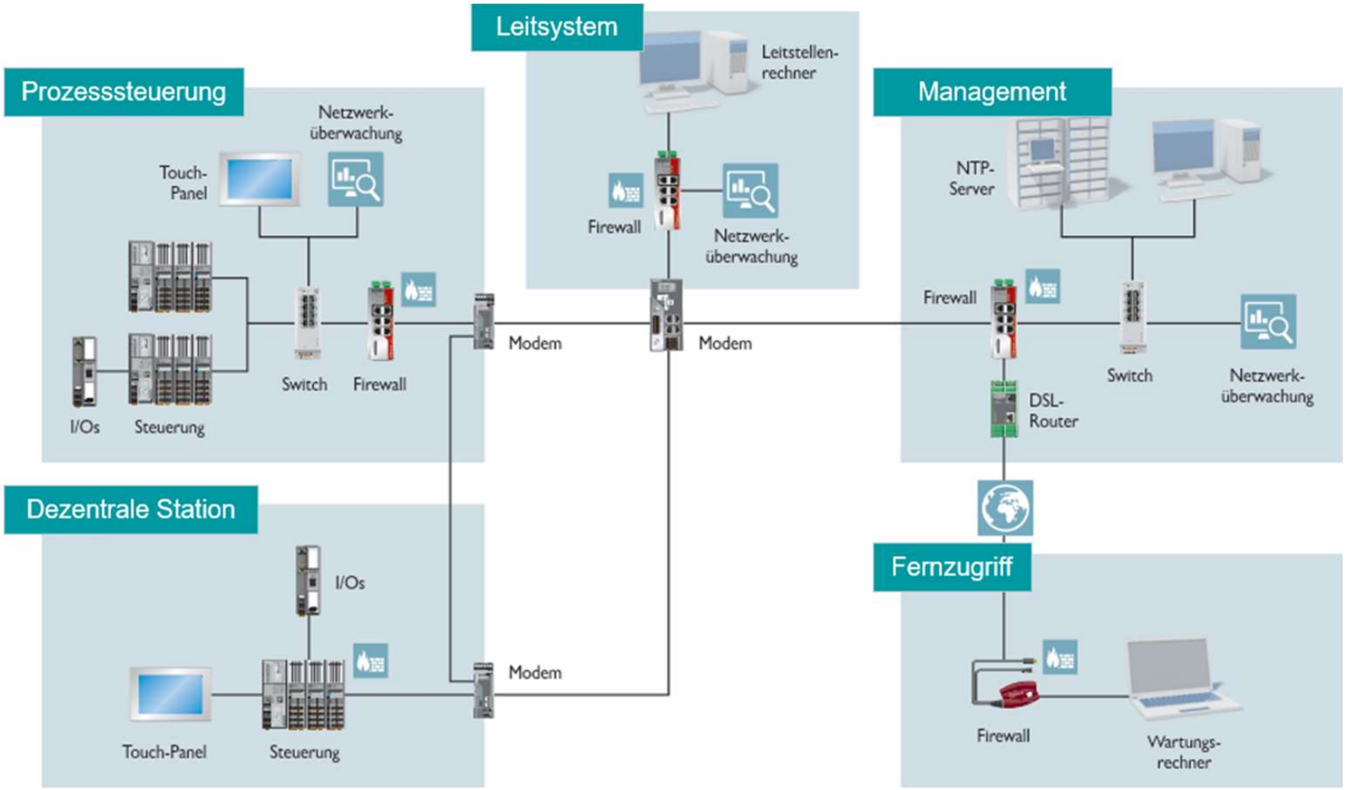
Production line

Production line

Machine

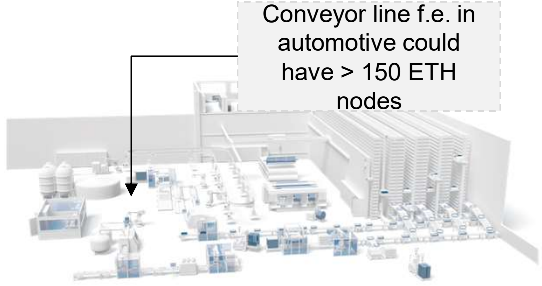
Digital Factory | Data Security | Security evaluation

Blueprint: Remote monitoring and control



Keep the control over your industrial network

Requirement

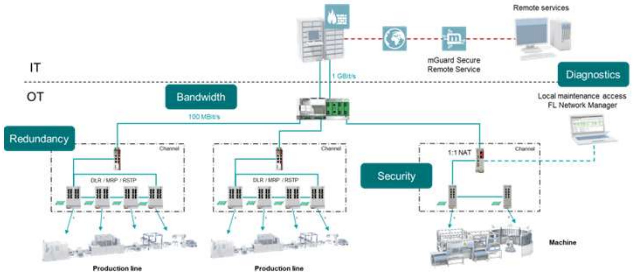


Conveyor line f.e. in automotive could have > 150 ETH nodes

Keeping the control over the industrial network

- Build a sustainable and resilient network infrastructure
- Reduce network errors and downtimes
- Simplify network maintenance
- Efficient connection between office and production network

Solution



„Smart automation network“

- Powerful network products
- Structured and intelligent network design
- Focus on:
  - Bandwidth
  - Redundancy
  - Diagnostics
  - Security

Result

Higher **network availability**

Combining the right network design with powerful components prevents system failures and downtimes leading to a higher system availability and cost reduction

Any Question